UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,311	06/28/2004	David Arditti Modiano	T2151-9156US01	9860

181 7590 11/28/2007

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
YALEW, FIKREMARIAM A	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
11/28/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipdocketing@milesstockbridge.com
sstiles@milesstockbridge.com

Office Action Summary	Application No.	Applicant(s)	
	10/500,311	ARDITTI MODIANO ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19-36,39 and 40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19-36,39-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The office action is in replay to an amendment filed on 09/04/2007.Claims 37-38 are cancelled. Claims 19-36 have been amended. Claims 39-40 are new added. Claims 19-36 and 39-40 are pending.

2. The examiner withdraws the previous U.S.C 101 claim rejection based on the applicant amendment.

Response to Arguments

4. Applicant's arguments with respect to claims 19-36 and 39-40 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 19-36 and 39-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over David Chaum (Group Signatures XP-000900793 04/1991) in view of Saito et al(hereinafter referred as Saito)US Patent No 6,161,183.

7. As per claim 19: David disclose a group signature device for providing a message (m) accompanied a group by a group signature (S) comprising means for producing the group signature(s) using the message(m) and the personalized data(Z,

Kz) such that a checker ,upon receiving the message(m) accompanied by the group signature(S),is able to verify that the message (m) is associated with the group (G) based on the personalized data(z, Kz) and the group signature (S), to authenticate the message (m) with the identity of the member (M) of the group(G) remaining anonymous to the checker(See page 1(i.e., cannot discover which group member made it)); and means for outputting the message(m) and the group signature (S) to the checker(page 1 abstract).

David does not explicitly teach means for storing personalized data (Z,Kz) identifying a member (M) of a group (G).

However Saito teaches means for storing personalized data (Z,Kz) identifying a member (M) of a group (G)(See col 5 lines 15-28 and Fig 1 step 11 and col 9 line 64 through col 10 line 8)

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to employ the teaching method of Saito within David inorder to enhance security of the device.

8. As per claim 20: the combination of David and Saito disclose a group signature device further comprising encryption means (B3) for producing personalizing encrypted text (C) using said personalized data (z; Kz) said means for producing the group signature(S) being configured to produce the signature(S) of the message (M) using said personalized encrypted text(C) the signature (S) of the message (m) using said personalized encrypted text(C)(See David page 259 first group signature scheme).

9. As per claim 21: the combination of David disclose a group signature device further comprising means (B5) for combining the message (m) to be signed and the encrypted text (C) associated with said message (m) in the form of a concatenation of the message (m) with the encrypted text (C)(See David pages 262-263 third group signature scheme).

10. As per claim 22: the combination of David and Saito disclose a group signature device wherein said means for producing the group signature (S) further comprises means (Sig-B6) for producing the group signature(S) of the message (m) using the encrypted text (C) associated with said message(m) (See Saito col 11 lines 46-67).

11. As per claim 23: the combination David and Saito disclose a group signature device wherein said personalized data is an identifier (z) personal to the member (M), said means for storing further includes an encryption key (K) common to all members of the group (G), and encryption means (B3) produces said encrypted text(C) using the identifier (z) and said encryption key (K) (See David page 258 i.e., same secret key).

12. As per claim 24: the combination of David and Saito disclose a group signature device in which encryption means (B3) produces said encrypted text (C) using identifier (z) and a random number (r)(See David page 259 first group signature scheme).

13. As per claim 25: the combination of David and Saito disclose a group signature device wherein said personalized data is a diversified encryption key (Kz) specific to each member (M) of the group (G), and encryption means (B3) produces said encrypted text (C) using at least one data and said diversified encryption key (Kz) (See Saito col 7 lines 1-12).

14. As per claim 26: the combination of David and Saito disclose a group signature device wherein said data includes a random number(r) (See Saito col 3 lines 47-58).

15. As per claim 27: the combination of David and Saito disclose a group signature device wherein the encryption means (B3) uses a secret key(K) and the Advanced Encryption Standard (AES) public encryption algorithm(See Saito col 3 lines 47-58).

16. As per claim 28: the combination of David and Saito disclose a group signature device wherein the encryption means (B3) uses one of the Rivest, Shamir, Adleman or Advanced Encryption Standard (AES) public encryption algorithms (See David page 258 i.e., RSA).

17. As per claim 29: the combination of David and Saito disclose a group signature device wherein the signature means (sig-B6) uses a private key signature algorithm (SK) (See Saito Fig 3 step 23).

18. As per claim 30: the combination of David and Saito disclose a group signature device which the private key signature algorithm is of Rivest, Shamir, Adleman(RSA) type.(See Saito col 5 lines 2-6).

19. As per claim 31: the combination of David and Saito disclose a group signature device in which said group signature device is a portable communicating device (26)(See Saito Fig step 12).

20. As per claim 32: the combination of David and Saito disclose a group signature device in which said portable communicating device is a smart card (26)(See Saito Fig 1 step 12).

21. As per claim 33: Saito discloses a method for secure communication of a message (m) sent by a member (M) of a group (G) using a group a signature (S) comprising producing the signature (S) of the message (m) with a private key (SK) common to members (M) of the group (G); integrating personalized data (z; KZ) in to the message (m);and verifying that the message(m) is associated with the group (G) based on the personalized data (z, KZ) and the group signature (S) to authenticate the message (m) without identifying the member (M) of the group(G)(See page 257-258).

David does not explicitly teach integrating personalized data (z; KZ) in to the message (m).

However Saito teaches integrating personalized data (z; KZ) in to the message (m)(See Figs 7A,7B).

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to employ the teaching method of Saito within David inorder to enhance security of the device.

22. As per claim 34: the combination of David and Saito disclose the method in which said verifying is performed using a public key corresponding to the said private key (SK) (See Saito col 11 lines 21-55).

23. As per claim 35: the combination of David and Saito disclose the method futher comprising the steps of: making correspondence data between the identities of members (M) of the group (G) and their personalized data available, before said producing the group signature(S); (See Saito col 7 lines 1-7,col 13 lines 56-64); decrypting the personalized data received from electronic device for which group

signature is to be opened(See Saito col 9 line 62 through col 10 line 8); and opening the group signature(S) if the decrypted personalized data corresponds to the identity of the member (M) of the group (G)(See Saito co 7 lines 1-7, col 13 lines 27-38).

24. As per claim 36: the combination of David and Saito disclose the method further comprising the steps of producing personalized data (z; Kz) associated with said electronic device to be personalized (See Saito Fig 6 and Fig 5 step 28); and registering said personalized data (z Kz) with a private signature key(SK) contained in said electronic device(See Saito Fig 6 and Fig 10 step s31).

25. As per claim 39: David discloses a group signature system for authenticating message (m) accompanied by a group signature (S), comprising: out put the message (m) and the group signature (S)(See page 257-258); a checker that receives that receives the message (m) accompanied by the group signature (S) output from the electronic device, said checker being configured to verify that the message (m) is associated with the group signature (S), the identify of the member (M) remaining anonymous to the checker; and a trusted authority configured to identify the member (M) of the group (G)(See page 257-258)

David does not explicitly disclose an electronic device configured to store personalized data (z,Kz) identifying a member (M) of group (G), to produce the group signature (S) using the message (m) and the personalized data (z,Kz)

Saito discloses an electronic device configured to store personalized data (z,Kz) identifying a member (M) of group (G), to produce the group signature (S) using the

message (m) and the personalized data (z,Kz)(See col 5 lines 15-28 and Fig 1 step 11 and col 9 line 64 through col 10 line 8)

Therefore it would have been obvious to one ordinary skill in the art at that time the invention was made to employ the teaching method of Saito within David inorder to enhance security of the system.

26. As per claim 40: the combination of David and Saito discloses a group signature system further comprising: a terminal including means for communicating with the electronic device (See Satio 10 lines 38-67); and a server provided in communication with terminal and the trusted authority (See Satio col 11 lines 45-67); wherein said trusted authority is provided in communication with a bank and a shopkeeper (See Satio col 11 lines 45-67).

Conclusion

27. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser,can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-272-4195.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew
11/20/07
FA

Art Unit 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/21/07